18/pets

-1-

ADDRESS BASED AUTHENTICATION SYSTEM AND APPARATUS AND PROGRAM THEREFOR

TECHNICAL FIELD

[0001] The present invention relates to an authentication system for a user terminal to receive a user authentication from an authentication server and to request a service offered by an application server on the basis of the authentication received, and in particular, to an authentication system in which upon a successful user authentication, the authentication server allocates a source address to the user terminal and the user requests a service offered by the application server using the allocated source address, and an apparatus and a program therefor.

BACKGROUND ART

[0002] When a user desires to obtain a service from a server through a network such as the internet, it is a general practice that a session be established between the terminal of the user (the user terminal) and the server and that a service request is sent to the server through the session. For the sake of charging for the service offered by the server, the latter requires a user authentication before the service is offered, and upon successful authentication, it offers the service through the established session. Thus, the user authentication takes place each time a service request to the server is made, and the service is offered through the established session. If the service offered covers a plurality of packets, the service is offered through the same session.

[0003] In view of an increased throughput experienced by each application server if a user authentication is performed in response to each service request, there is proposed a method in which a user authentication is performed by an authentication server, which upon successful authentication, allocates an IP address to the user, who then requests the server for a service to be offered using the IP address as a source address.

In the prior art network authentication system, such an address based authentication method as indicated below is disclosed in patent literature1, for example. Specifically, when a user utilizes a connection service, a network access authentication server refers to a personal information database in which a correspondence between a customer information and a user ID (information which uniquely identifies a user) is pre-stored in order to authenticate the user, and upon successful authentication, allocates an IP (Internet Protocol) address to the user's terminal together with a connection grant, transmits the allocated IP address to the user terminal while concurrently storing the relationship between the IP address and the user ID in a storage, and when utilizing a commercial transaction service, the user terminal proposes a purchase of goods to a sales service provider apparatus on the internet using the IP address transmitted from the network access authentication server, the sales service provider address obtains the source IP address of a goods purchase proposal packet and sends this IP to the network access authentication server for inquiry and acquires the user ID on the basis of the IP address and then acquires the customer information which corresponds to the acquired user ID for purpose of authenticating the customer.

Patent literature 1: JP Application Kokai Publication No. 2002-207929

DISCLOSURE OF THE INVENTION

ISSUES TO BE SOLVED BY THE INVENTION

[0004] However, the prior art authentication system mentioned above presents a problem that during the network access authentication of the user or while the service is being provided, a third party may eavesdrop the IP address used by the user from the packet which is transmitted or received on the network to enable impersonation by accessing the server which provides the commercial transaction service. In other words, the prior art address based authentication system cannot guarantee the authenticity of the address allocated to the user. It is to be noted that an authentic address refers to an address which an organization such as ISP (internet service provider) allocates to a user or user terminal according to a correct procedure.

[0005] It is an object of the present invention to provide an address based authentication system, an apparatus and a program therefor which can guarantee the authenticity of an address allocated to a user in order to overcome such a problem of the prior art.

MEANS TO SOLVE ISSUES

[0006] In accordance with the present invention, in an authentication system in which an authentication server which authenticates a user, a user terminal which transmits a user authentication information and an application server which provides a service to a user through the user terminal are connected together in a manner to permit a communication therebetween;

the authentication server

authenticates a user on the basis of user authentication information transmitted as an authentication request from the user terminal by utilizing authentication means, and upon a successful authentication of the user, allocates an address to the user terminal by an address allocation means, issues a ticket including the allocated address by a ticket issuing means and transmits the issued ticket to the user terminal;

the user terminal

transmits the user authentication information to the authentication server, receives the ticket transmitted from the authentication server, sets up the address contained in the ticket as a source address for a packet which is transmitted from the user terminal by a source address set-up means, transmits a packet including the ticket to the application server, and transmits a packet which represents a request for a service to the application server by a service request means;

and the application server

stores the ticket transmitted from the user terminal in a ticket memory means, determines by an address comparison means whether or not the source address of the packet representing a request for a service which is transmitted from the user terminal coincides with the address contained in the ticket stored in the ticket memory means, and upon determining that the addresses coincide, transmits a packet which provides a service to the user to the user terminal by a service providing means.

EFFECTS OF THE INVENTION

[0007] With the described arrangement, the authentication of a user and the allocation of an address are performed by the same authentication server and accordingly, it is assured that an address be allocated only to a valid user. Since the same authentication server performs the allocation of an address and an issuing of a ticket, the authenticity of the address can be guaranteed by the ticket.

Since the address is issued on the basis of the user authentication, the authenticity of the address can be guaranteed. In addition, the transmission of the ticket to the application server takes place only once, and since the address contained in this ticket is one which is given by the authentication server to the user terminal for which the valid user has just requested its authentication and since the address in this ticket is treated as the source address, it follows that if the source address of each service request packet which is transmitted from the user terminal through the session which is established for the transmission of the ticket coincides with the address contained in the stored ticket, that packet can be regarded as the packet from the authenticated user. Thus, the source address of the service request packet is associated with the authenticated user through the address contained in the ticket which is sent only once during the time the session is established. If a third party eavesdrops the source address of the service request packet and uses it to make a service request to the application server, the address contained in the stored ticket cannot coincide with the source address during that session, preventing a service from being provided.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Fig. 1 is a block diagram showing an exemplary system arrangement of an authentication system according to a first and a second mode for carrying out the present invention;

Fig. 2 is a block diagram showing an exemplary functional arrangement of an authentication server according to the first mode for carrying out the present invention;

Fig. 3 is a block diagram showing an exemplary functional arrangement of a user terminal according to the first mode for carrying out the present invention;

Fig. 4 is a block diagram showing an exemplary functional arrangement of an application server according to the first mode for carrying out the present invention;

Fig. 5 is a view showing an example of construction of a ticket used in the first mode for carrying out the present invention;

Fig. 6 is a view showing an example of construction of a packet including a ticket which is used in the first mode for carrying out the present invention;

Fig. 7 is a sequence diagram showing an exemplary processing procedure of the authentication system according to the first mode for carrying out the present invention;

Fig. 8 is a flow chart showing an exemplary flow of processings by the authentication server according to the first mode for carrying out the invention;

Fig. 9A is a flow chart showing an exemplary flow of processings which occur during a user authentication at a user terminal according to the first mode for carrying out the present invention;

Fig. 9B is a flow chart showing an exemplary flow of processings which occur during a service request;

Fig. 10 is a flow chart showing an exemplary flow of processings by the application server according to the first mode for carrying out the present invention;

Figs. 11A and 11B illustrate examples of a different functional arrangement of authentication information generating means 151 shown in Fig. 2;

Fig. 11C illustrates an example of a different functional arrangement of an authentication information verifier 320a shown in Fig. 4;

Fig. 12 is a block diagram showing an exemplary functional arrangement of an authentication server according to the second mode for carrying out the present invention;

Fig. 13 is a block diagram showing an exemplary functional arrangement of a user terminal according to the second mode for carrying out the present invention;

Fig. 14 is a block diagram showing an exemplary functional arrangement of an application server according to the second mode for carrying out the present invention;

Fig. 15 is a view showing an example of construction of a ticket which is used in the second mode for carrying out the present invention;

Fig. 16 is a view showing an example of construction of a packet added with an authentication header which is used in the second mode for carrying out the present invention;

Fig. 17 is a sequence diagram showing an exemplary processing procedure of the authentication system according to the second mode for carrying out the present invention;

Fig. 18 is a flow chart showing an exemplary flow of processings by the authentication server according to the second mode for carrying out the present invention;

Fig. 19A is a flow chart showing an exemplary flow of processings which occur in the user terminal during the user authentication according to the second mode for carrying out the present invention;

Fig. 19B is a flow chart showing an exemplary flow of processings during a service request;

Fig. 20 is a flow chart showing a exemplary flow of processings by the application server according to the second mode for carrying out the present invention;

Fig. 21A is a sequence diagram showing an exemplary processing procedure in the authentication system when another example of key information is used;

Fig. 21B is a block diagram showing a specific example of a challenge generator which is added to the authentication server shown in Fig.

12.

Fig. 21C is a block diagram showing another specific example of a key information generator shown in Fig. 13; and

Fig. 21D is a block diagram showing a specific example of a modification within a ticket verifier means 620 shown in Fig. 14.

BEST MODES FOR CARRYING OUT THE INVENTION

[0009] Several modes for carrying out the present invention will now be described in detail with reference to the drawings. In the description to follow, corresponding parts are designated by the same reference characters while avoiding a duplicate description.

[First mode] system arrangement

Fig. 1 is a view of a system arrangement of an address based authentication system according to the first mode for carrying out the present invention. The address based authentication system according to the present invention comprises an authentication server 100 which authenticates a user, an access point 30 which covers a plurality of user terminals 200 which transmit user authentication information, and a plurality of application servers 300 which transmit a packet which provides a service to the user to the user terminals 200, all of which are connected together in a manner to permit a communication therebetween through a network 10.

[0010] The authentication server 100 is connected with a user database 20 which stores information relating to users (user authentication data). A user is not limited to a user which operates a user terminal 200, but may also be a program itself which acts as an operator, for example, which may appear as if a user is utilizing a user terminal during the execution of a program in a computer. The address based authentication system may be arranged such that the security of the network between the user terminals 200 and the application servers 300 is physically secured. In this instance, there is no need for a processing which confirms whether or not a packet transmitted from the user terminal 200 to the application server 300 is forged.

[0011] The network 10 may comprise a wireless or wired network, LAN (Local Area Network) or the internet. The access point 30 may be provided for each given area. The user terminal 200 may comprise a cell phone, hand set, personal appliance or a personal computer which is capable of a wireless communication. The application server 300 may comprise a server which provides a contents distribution service including a movie and sports programs, an electronic commercial transaction service, a communication service for electronic mail, IP telephone and instant messaging, or information browser service such as World Wide Web. In addition, the application server 300 may also comprise a gateway server or a firewall which provides an access to services on a separate network.

[0012] The user terminal 200 requests an authentication of a user by transmitting user authentication information which is required to have the user authenticated by the authentication server 100 through the access point 30. In this mode of carrying out the invention, the user authentication information includes at least one of a user identifier and a password, information generated on the basis of a key pair in order to authenticate a user, biometrics of a user (for example, fingerprint, iris, vein pattern, holograph, voice print, or the like), and other information used in known various technologies of user authentication. It will be noted that a key pair represents a pair of an public key and a private key which are based on the public key cryptography.

[0013] The authentication server 100 authenticates a user by referring to the user database 20 on the basis of user authentication information which is transmitted from the user terminal 200, and upon a successful authentication of the user, allocates a user identifier which corresponds to the user, and allocates an address which is capable of uniquely identifying a user terminal which corresponds to the allocated user identifier, issues a ticket including the allocated address and user identifier, and transmits the issued ticket to the user terminal 200.

The user terminal 200 uses the address contained in the ticket transmitted from the authentication server 100 as a source address for a packet which is transmitted from the user terminal 200, and initially transmits the ticket to the application server 100, followed by transmitting a packet which requests a service (hereafter referred to as a service request packet).

[0014] The application server 300 stores the ticket transmitted from the user terminal 200, determines whether or not the address contained in the stored ticket coincides with the source address of the service request packet, and upon determining a coincidence of the addresses, transmits a packet which provides a service to the user to the user terminal 200.

[First mode] authentication server

Fig. 2 is a block diagram of an authentication server which is used in the first mode for carrying out the invention. The authentication server 100 comprises a communication interface 101 and control processing means 102. The communication interface 101 may comprise a modem or LAN interface, for example, and any means may be used to construct it provided it enables a communication with a communication equipment connected with the network 10.

[0015] The control processing means 102 comprises a control unit 102a including a CPU (Central Processing Unit) which executes a program, a memory which stores the program and the like, user authentication information reception means 110, authentication means 120, a user identifier allocating means 130, an address allocating means 140, a ticket issuing means 150 and a ticket transmitting means 160. It should be understood that these means need not be constructed as hardwares, but may function by the execution of a program.

The authentication server 100 mentioned above is connected to a user database 20 which stores information relating to users, and the user database 20 has user ID entry data in storage which includes authentication data which is used when authenticating a user and a user ID's (such as a name or information which uniquely identifies a user by itself).

[0016] The user authentication information reception means 110 receives an authentication request inclusive of user authentication information which is transmitted form the user terminal 200 through the communication interface 101.

The authentication means 120 performs an authentication of a user on the basis of user authentication information of the authentication request which is received by the user authentication information reception means 110. The authentication means 120 authenticates a user by verifying a consistency between the user authentication information and the authentication data stored in the user database 20.

Upon a successful authentication of a user, the user identifier allocating means 130 allocates a user identifier ID_U corresponding to that user in response to the authentication request. It is to be understood that a user identifier is a unique identifier in the address based authentication system . Alternatively, the user identifier ID_U may be an expandable one which fulfils the uniqueness globally such as "A@B" where A represents a unique identifier within the authentication server and B a global IP address of the authentication server. Thus, the user identifier corresponds to a user uniquely in a set of assumed users. However, a single user may correspond to a plurality of user identifiers concurrently.

[0017] The user identifier allocating means 130 acquires a user ID from user ID entry data which is stored in the user database 20, for example, and allocates the acquired user ID as a user identifier ID_U in response to the authentication request. Alternatively, the user identifier allocating means 130 may generate a random number in an encryption means 140a when it has acquired a user ID, add the generated random number to the acquired user ID, and a resulting (random number + user ID) information may be further encrypted with an identifier generating secret key of the authentication server 100 to be allocated as a user identifier ID_U. When arranged in this manner, only a person who knows the identifier generating secret key, for example the authentication server 100 is in a position to know the user ID on the basis of the user identifier ID_U, whereby the privacy protection of the user can be realized even though the user identifier ID_U is contained in a ticket to be transmitted to the application server. As a further alternative, the user identifier allocating means 130 may allocate a user identifier ID_U from the user authentication information or may choose something from random numbers, characters, a sequence number, which can be uniquely associated with the user ID by the database.

[0018] An address allocating means 140 allocates an address A_U to a user terminal which corresponds to the user identifier ID_U which is allocated by the user identifier allocating means 130. This address A_U may be an IP address and in addition may be a mail address, URI (Uniform Resource Identifier) used in SIP (Session Initiation Protocol) or an addressee of IM (Instant Messaging).

If it can be assumed that during the address allocation by the address allocating means 140, a correspondence of a same address to a plurality of user identifiers simultaneously cannot occur, one address uniquely corresponds to a user identifier and also uniquely corresponds to a user.

[0019] In order to allow a correspondence between the user identifier ID_U allocated to the authenticated user and the allocated address A_U to be readily recognizable, such correspondence or a ticket itself which contains such correspondence information is stored in an allocation memory 102b or in association with user information contained in the user database 20. The user identifier ID_U and the address A_U which are allocated to the same user may be changed each time an authentication request is made. For this reason, tickets for the same user are distinguished according to the date and the time when the tickets have been issued. User identifiers ID_U and addresses A_U which fall into disuse are deleted at suitable times. In this manner, an accommodation is made to answer an inquiry from the application server 300 about the user information or to charge for the service provided, on the basis of the user identifier ID_U.

[0020] Ticket issuing means 150 includes authentication information generating means 151 in this example, temporarily generating a provisional ticket (ID_U, A_U) containing the user identifier ID_U allocated by the user identifier allocating means 130 and the address A_U allocated by the address allocating means 140, generating authentication information IA on the basis of the provisional ticket by the authentication information generating means 151, and issuing a ticket CK1 containing the authentication information IA, the user identifier ID_U and the address A_U.

As illustrated in Fig. 5, the ticket CK1 consists of the user identifier, the address, authentication information and in addition, a time stamp representing the date and time when the ticket CK1 has been issued, information representing an effective period of the ticket, and while not shown in Fig. 5, information representing a communication band width allocated to the user terminal 200, and information relating to the access point 30 which covers the user terminal 200, for example, positional information or the like. When the time stamp is contained, the ticket issuing means 150 includes a clock section 150a, and a time stamp delivered from the clock section 150a is utilized. Information representing the effective period of the ticket and the information representing the communication band width allocated to the user terminal 200 may be previously determined by a contract between the user who uses the user terminal 200 and application service providers or a communication enterprise which operate the access points 30, the authentication server 100 and the application servers 300. .

[0021] In addition, an authentication server identification information (for example, address A_A) which uniquely identifies the authentication server 100 may be contained in the ticket CK1 as shown in Fig. 5, for example. Alternatively, where the identifier A which is unique within the authentication server 100 and the global IP address of the authentication server 100 are combined into the form "A@B" to be used as the user identifier ID_U, as mentioned previously, this B may be used as the authentication server identification information, as indicated in Fig. 5.

The authentication information generating means 151 inputs a shared secret key K_{CAS} which is shared beforehand with the application server 300 and the provisional ticket (ID_U, A_U), then calculates one-way hash function with respect to the provisional ticket using the shared secret key K_{CAS} to generate a authenticator MAC (message authentication code), which is delivered as authentication information IA.

[0022] The ticket transmitting means 160 transmits the ticket 51 issued by the ticket issuing means 150 to the user terminal 200 through the communication interface 101.

[First mode] user terminal

Fig. 3 is a block diagram of a user terminal used in the first mode for carrying out the present invention. The user terminal 200 comprises a communication interface 201 and control processing means 202. The communication interface 201 comprises either a wired or wireless LAN interface, a modem or a communication instrument such as a cellphone(module) or the like, and any interface may be used which is capable of a communication with a communication equipment connected with the network 10 through the access point 30.

[0023] The control processing means 202 comprises a control unit 202a including a CPU which executes a program, a memory which stores the program and the like, an authentication request means 203 and a service request means 230. The functions of these means may be served by modules of the program or by the execution of the program as in the authentication server 100. The authentication request means 203 comprises user authentication information generating means 210, user authentication information transmitting means 220 and ticket reception means 231.

The user authentication information generating means 210 generates a user authentication information including information which represents a user name and a password. The user authentication information generating means 210 responds to an entry of a user name and a password from an entry instrument 40 such as a keyboard, for example, by generating user authentication information in accordance with the entered information. Alternatively in place of the user name and the password, at least one of the following information required by the authentication server 100 in order to authenticate a user, is used for the user authentication information, information generated on the basis of the key pair for authentication the user, information which authenticates biometrics of the user, etc., which are used in known methods of the user authentication.

[0024] The user authentication information transmitting means 220 transmits the user authentication information which is generated by the user authentication information generating means 210 to the authentication server 100 through the communication interface 201 for purpose of authentication request.

The ticket reception means 231 receives a packet including the ticket (CK1) 51 transmitted from the authentication server 100 through the communication interface 201, and the address A_U contained in the received ticket 51 is set up and registered as a source address A_S in the communication interface 201, for example, in a register 201a by a source address set-up means 231a. Alternatively, an address contained in the ticket 51 received by a source address set-up means 230a of the service request means 230 may be set up and registered as a source address A_S in the register 201a within the communication interface 201.

[0025] The service request means 230 includes a session establishing means 232, requesting a service to be provided by the application server 300.

The session establishing means 232 establishes a session between the application server 300 and the user terminal 200 depending on the service utilized by the user. For example, the session establishing means 232 establishes a session by transmitting the ticket (CK1) 51 received by the ticket reception means 231 to the application server 300 through the communication interface 201 at some step during the processing operation to establish the session. A session establish request packet 52 consists of a header portion

52h including the source address A_S and a payload portion 52p including the ticket 51, as illustrated in Fig. 6, for example.

[0026] For example, the session establishing means 232 transmits the packet 52 to the application server 300 through the communication interface 201. The communication interface 201 sets up the address A_S which is registered by the source address set-up means 231a of the ticket reception means 231 as a source address of the packet 52 and transmits the packet 52. The service request means 230 transmits packets representing a service request (service request packets) to the application server 300 during the established session using the address registered in the communication interface 201 as the source address A_S.

[0027] [First mode] application server

Fig. 4 is a block diagram of an application server which is used in the first mode for carrying out the invention. An application server 300 comprises a communication interface 301 and a control processing means 302. The communication interface 301 may comprise a modem or LAN interface, for example, and any interface may be used provided it enables a communication with a communication equipment connected to the network 10.

The control processing means 302 comprises a control unit 302a including a CPU which processes a program, a memory which stores the program and the like, a service providing means 310, a session establishing means 311 and a ticket memory means 330. In the similar manner as in the authentication server 100, these means may be served by modules of the program.

[0028] The service providing means 310 includes an address comparison means 312, and provides a service which is requested by the user terminal

200.

The session establishing means 311 includes a ticket verifying means 320, and establishes a session with the user terminal 200. In the procedure to establish a session, the session establishing means 311 receives a packet 52 including the ticket (CK1) 51 transmitted from the user terminal 200.

The ticket verifying means 320 verifies whether or not the ticket (CK1) 51 contained in the packet 52 is forged. The ticket verifying means 320 verifies the authentication information IA contained in the received ticket 51 in an authentication information verifier 320a, for example. Specifically, if authentication information IA is an authenticator(MAC: message authentication code), it verifies whether or not the ticket 51 has been forged in the authenticator verifier 320a using a shared secret key K_{CSA} which is previously shared with the authentication server 100. In addition, the ticket verifying means 320 collates the address A_U contained in the ticket 51 against the source address A_S in the packet 52 in an address collator 320b, and if they do not coincide, the verification fails.

[0029] In addition, if the ticket (CK1) 51 contains the effective period EPe, the ticket verifying means 320 may verify whether or not the ticket 51 is within its effective period in an effective period verifier 320f in accordance with a time information from the clock section 320d. The ticket verifying means 320 may perform a verification by choosing shared secret keys which are individually prepared for each period according to a value in the time stamp Tms contained in the ticket (CK1) 51. When the time stamp Tms is contained in the ticket (CK1) 51, the ticket verifying means 320 may verify whether or not the ticket 51 is effective according to a time information from the clock section 320d and the date and the time the ticket has been produced as represented by the time stamp. Alternatively, the effective period verifier 320f may verify whether or not a service requested by the user based on the time stamp contained in the ticket 51 and the information representing the effective period is within the effective providing period of the service providing means 310.

[0030] When a result of the collation of the address A_U contained in the ticket (CK1) 51 and the source address A_S of the packet 52 performed by the ticket verifying means 320 indicates a match and it is determined that the ticket has been transmitted from a user terminal having the authentic address, this ticket 51 is stored in the ticket memory means 330. However, if any one of other verifications and collations performed by the ticket verifying means 320 is unsuccessful, the ticket 51 is prevented from being stored in the ticket memory 320a. For example, outputs from the detectors 320a, 320c, and 320d and the collator 320b are input to a memory command unit 320g, and if any one of the inputs indicates unsuccessful, a command to store the ticket 51 is not generated.

[0031] The address comparison means 312 verifies whether or not the source address A_S coincides with the corresponding address A_U which is contained in the ticket 51 by referring to the ticket memory means 330 in accordance with the source address A_S of the packet representing the service request. When the address A_U contained in the ticket 51 coincides with the source address A_S of the packet, the service providing means 310 transmits to the user terminal 200 packets which are effective to provide a service requested by the user terminal 200 to the user.

If required, the service providing means 310 may make an inquiry based on the user identifier ID_U contained in the ticket 51 to the authentication server 100 about the user information. In addition, the service providing means 310 may transmit an information relating to the charge involved with the service provided to the user database 20 through the authentication server 100. In this instance, if the ticket CK1 contains the identification information of the authentication server 100, as shown in Fig. 5, the authentication server can be specified if there exist a plurality of authentication servers, and if authentication server identification information is an address (for example, an address A_A), this address may be used to access the authentication server 100 immediately.

[0032] [First mode] processing procedure of the authentication system

A processing procedure of the address based authentication system according to the first mode for carrying out the invention will now be described with reference to Fig. 7.

(1) Initially, when the authentication of the user is requested to the authentication server, the user terminal 200 prepares user authentication information, which is then transmitted through the access point 30 to the authentication server 100.

(2) Upon receiving the authentication request, the authentication server 100 performs an authentication of the user on the basis of the user authentication information. Upon a successful authentication of the user, the authentication server 100 allocates a user identifier ID_U to the user, allocates an address A_U to the user terminal 200 which corresponds to the user, and issues a ticket 51 containing an authentication information IA for the allocated address A_U, a time stamp, and an effective period and the like as required, and

(3) transmits the ticket 51 to the user terminal 200.

[0033] (4) Upon receiving the ticket 51, the user terminal 200 sets up the address of the ticket 51 as a source address A_S, and transmits a packet 52 including the ticket 51 to the application server 300, thus requesting a session with the application server 300 to be established.

(5) Upon receiving the packet 52, the application server 300 verifies the correctness of the ticket according to the authentication information, and upon a successful verification, collates the source address A_S of the packet against the address A_U contained in the ticket 51, and if they match, stores the ticket 51 and establishes a session.

[0034] (6) When the session is established, the user terminal 200 transmits service request packets to the application server 300 through the established session.

(7) Upon receiving these service request packets, the application server 300 determines whether or not the source address A_S of the service request packet coincides with the address A_U contained in the stored ticket 51, and upon coincidence between the addresses, it transmits a packet which is effective to provide the service to the user to the user terminal 200.

[First mode] processing by the authentication server

Fig. 8 is a flow chart showing a flow of processings by the authentication server 100 which is used in the first mode for carrying out the invention.

[0035] Initially, the authentication information which is transmitted from the user terminal 200 is received through the communication interface 101 by the user authentication information reception means 110 (S101) and an authentication of the user is made by the authentication means 120 on the basis of the user authentication information, and upon a successful authentication of the user, the operation proceeds to S103, while upon an unsuccessful authentication of the user, the operation is terminated (S102).

Upon a successful authentication of the user, the address A_U is allocated to the user terminal 200. In this example, a user identifier ID_U

corresponding to the user is allocated by the user identifier allocating means 130 (S103), and an address A_U is allocated by the address allocating means to the user terminal which corresponds to the user identifier ID_U (S104).

[0036] Then a provisional ticket which includes the user identifier ID_U allocated by the user identifier allocating means 130 and the address A_U allocated by the address allocating means 140 in this example is temporarily produced by the ticket issuing means 150, and using a shared secret key which is beforehand shared with the application server 300, the authentication information generating means 151 generates an authenticator MACfor the provisional ticket (S105).

A ticket 51 containing the user identifier ID_U, the address A_U and the authenticator MACor the like is then issued by the ticket issuing means 150 (S106), and the ticket 51 is transmitted by the ticket transmitting means 160 to the user terminal 200 through the communication interface 101 (S107).

[0037] [First mode] processing by the user terminal

Figs. 9A and 9B are flow charts showing a flow of processings by the user terminal 200 which is used in the first mode for carrying out the invention.

Initially, as shown in Fig. 9A, a user authentication information including information representing a user name and a password is generated by the user authentication information generating means 210 (S201), and the user authentication information is transmitted by the user authentication information transmitting means 220 to the authentication server 100 through the communication interface 201 (S202).

[0038] The ticket 51 transmitted from the authentication server 100 is received by the ticket reception means 231 (S203).

As shown in Fig. 9B, after the ticket 51 has been received, a session with the application server 300 is established by the session establishing means 232 (S204). After a session with the application server 300 has been established, packets representing a service request are transmitted by the service request means 230 to the application server 300 through the session (S205).

[0039] [First mode] processing by the application server

Fig. 10 is a flow chart showing a flow of processings by the application server 300 which is used in the first mode for carrying out the present invention.

Initially, the establishment of a session of the user terminal 200 is initiated by the session establishing means 311 (S301), and the ticket 51 contained in the packet 52 is received by the application server 300. The ticket 51 is verified by the ticket verifying means 320, and when the ticket 51 is verified to be authentic, the operation proceeds to S303 while if the ticket 51 is verified to be not authentic as by being forged, the operation is terminated (S302).

[0040] When the ticket 51 is verified to be authentic, a session is established by the session establishing means 311 and the ticket 51 is stored in the ticket memory means 330 (S303). A packet requesting service which is transmitted from the user terminal 200 is received, and the address comparison means 312 determines whether or not the source address A_S of the packet and the address A_U contained in the stored ticket 51 coincide (S304), and when a coincidence of the addresses is determined, packets which enable the service to be provided to the user by the service providing means 310 through the user terminal 200 is transmitted (S305). If the source address A_S and the address A_U do not coincide, the operation is terminated.

[0041] As described above, the address based authentication system according to the first mode for carrying out the present invention issues an address on the basis of the user authentication, and accordingly, it is guaranteed that the address has been issued to an authentic user (user identifier). In view of this relationship, the authentication server 100 issues the ticket 51 containing the allocated address and user identifier, the user terminal transmits the issued ticket 51 to the application server, and the application server 300 verifies and stores the transmitted ticket 51 and collates the source address of the service request packet which is transmitted from the user terminal 200 against the address contained in the stored ticket 51, and upon finding a coincidence therebetween, regards the service request packet as a packet from the authenticated user. In this manner, the address based authentication is enabled.

[0042] In other words, the ticket issued by the authentication server on the basis of the user authentication guarantees a correspondence between the user (identifier) and the address, and accordingly, by collating the source address A_S of the service request packet against the address A_U in the stored ticket, it is possible to confirm whether or not this packet has come from the authenticated user.

In this mode, the authenticity of the ticket 51 is verified by using an authentication information which is generated using a shared secret key which is beforehand shared between the application server 300 and the authentication server 100, and accordingly, it is possible to guarantee the authenticity of the ticket 51 issued by the authentication server 100, in particular, the authenticity of the address contained therein.

[0043] Also in this mode, the authentication server 100 issues the ticket 51 containing information which represents the effective period of the ticket 51 and the application server 300 verifies the validity of the ticket 51 in terms of the effective period, allowing the effective period to be determined in accordance with the principle of operation of the authentication server 100.

[First mode] modification

The user identifier allocating means 130 is not always required in the authentication server 100. The user identifier may be omitted as one of elements of construction of the issued ticket 51. In this instance, the user identifier allocating means 130 is omitted, and as indicated in broken lines in Fig. 8, upon a successful authentication at S102, the operation immediately transfers to step S104. However, when the user identifier is used, the ticket 51 itself provides a correspondence between the address A_U allocated to the user terminal 200 and the user, whereby the application server 300 can make an inquiry about the user information to the authentication server 100 using the user identifier. When the user identifier is omitted, it is necessary that this inquiry be made by using the address A_U and the authentication server 100 is required to store a correspondence between the address A_U allocated to the user terminal and the user ID.

[0044] The authentication information IA generated by the authentication information generating means 151 is not limited to the authenticatorMAC. As illustrated in Fig. 11A, for example, the provisional ticket (ID_U, A_U) may be input to a signature calculator 151b to perform a digital signature calculation with respect to the provisional ticket (ID_U, A_U) using the private key K_{SA} of the authentication server 100 which is based on the public key cryptography to generate a signature, which may be used as the authentication information IA. Alternatively, as illustrated in Fig. 11B, the provisional ticket (ID_U, A_U) which is input to the authentication information generating means 151 may be encrypted in an encryptor 151c using the secret key K_{CAS} shared with the application server 300, and the encrypted provisional ticket may be used as authentication information IA.

[0045] Where a signature is used as the authentication information IA, the authentication information verifier 320a within the application server 300 will be a signature verifier rather than the authenticator verifier, as indicated in parentheses in Fig. 4, and the signature as the authentication information IA is subject to a signature verification with the public key K_{PA} of the authentication server 100. If the entire ticket 51 is encrypted to be used as the authentication information IA, the authentication information verifier 320a is constructed as shown in Fig. 11C where the authentication information IA is decrypted in a decryptormeans 320a1 using the shared secret key K_{CAS} with the authentication server 100, and a decrypted result is collated against the provisional ticket (ID_U, A_U) in the collator 320a2, leading to a successful verification for the coincidence therebetween.

[0046] Where the user identifier is not used as one element of the ticket 51, the provisional ticket comprises only the address A_U. Where the time stamp or the like is contained as an element of ticket 51, it is treated as a part of provisional ticket, and the authentication information IA for the provisional ticket is prepared. In sum, every element other than the authentication information IA in the ticket 51 may be treated as a provisional ticket to prepare the authentication information IA.

The authentication information IA in the ticket 51 may be omitted. Thus, as indicated in broken lines in Fig. 8, the operation may directly transfer from step S104 to S106. However, when the authentication information IA is used, the verification of the ticket which takes place at step S302, indicated in broken lines in Fig. 10 and which takes place in the application server 300, initially verifies the authentication information IA to verify whether or not the provisional ticket is forged (S302a), and when it is confirmed that the ticket is not forged, and accordingly the address A_U contained in the ticket 51 is not forged, but is authentic, the source address A_S is collated against the address A_U in the ticket to see if the both addresses coincide (S302b), and upon coincidence, the operation transfers to S303, while the operation is terminated for a non-coincidence.

[0047] As elements in the ticket 51, either one or both of the time stamp and the effective period may be omitted. In the application server 300, each time a session with the user terminal 200 is established, the ticket CK1 of the packet which is received from the user terminal 200 may be immediately stored in the ticket memory means 330. Thus, the ticket verifying means 320 shown in Fig. 4 may be omitted, and the operation may proceed from the processing S301 directly to the processing S303 as indicated in broken lines 31 in Fig. 10. Even if a change is made in this manner, the transmission of the ticket CK1 takes place only once from the user terminal to the application server 300 each time a session is established, and because the user authentication takes place by the authentication server each time the user terminal requires a new service and the address (the address contained in the ticket CK1) which is then allocated to the user terminal 200 changes, thus it is difficult that a third party impersonates the user by eavesdroppping the source address A_S.

[0048] The user database 20 is not always required to be connected to the authentication server 100. For example, when the user authentication takes place using the public key cryptography, there is no need for authentication data. However, in order to confirm that a user public key certificate which is transmitted from the user terminal 200 is reliable, an inquiry is made to the public key certificate issuing organization which has issued the public key certificate, and if it is authentic, the user information contained in the public key certificate is acquired, and if it is insufficient, a database within the public key certificate issuing organization acquires information concerning a corresponding user.

The authentication server 100 may be constructed with a group of servers which are connected together through a secure network and which have a dependable relationship relative to each other. For example, it may comprise a devoted authentication server, an address issuing server, a ticket issuing server and the like which are connected together through a secure network.

[0049] [Second mode] arrangement of authentification system

A second mode for carrying out the present invention will now be described, with the description principally dealing with a distinction from the first mode. In the second mode also, an authentication server, user terminals and application servers are provided and although they have different functions from the first mode, the system arrangement is similar to the first mode shown in Fig. 1, and accordingly, reference numerals used in the second mode are indicated in parentheses in Fig. 1. An authentication server 400, user terminals 500 and application servers 600 are connected in a manner to permit a communication therebetween through the network 10.

[0050] In the second mode, a user terminal 500 transmits a key information in addition to user authentication information when it requests an authentication by an authentication server 400. Thus, the user terminal 500 has key information. Key information includes information relating to an public key of a user or a user terminal such as a public key of a user key pair, a public key of a terminal key pair, a certificate including such public key, or hashed value which is obtained by applying one-way hash function to the public key or the certificate including the public key.

When issuing a ticket upon a successful user authentication in response to an authentication request from a user terminal 500, in the second mode, the authentication server 400 causes key information transmitted from the user terminal to be contained in the ticket in addition to the user identifier and the address.

[0051] [Second mode] authentication server

Fig. 12 is a block diagram of an authentication server which is used in the second mode for carrying out the present invention. The authentication server 400 comprises a communication interface 101 and a control processing means 402.

The control processing means 402 comprises a control unit 402a including a CPU (Central Processing Unit) which processes a program and a memory which stores the program and the like, a user authentication information reception means 110, an authentication means 420, a user identifier allocating means 130, an address allocating means 140, a ticket issuing means 450 and a ticket transmitting means 160. It should be understood that these means may be constructed by modules of the programs.

[0052] The authentication means 420 performs an authentication of the user on the basis of user authentication information which is received by the user authentication information reception means 110. By way of example, the authentication means 420 verifies a matching between the user authentication information and authentication data stored in the user database 20 in an authentication information collator 120a for purpose of user authentication. If required, the authentication server may also confirm whether or not a user terminal keeps a private key related to a key information IK. For example, the possession of a private key which forms a pair with an public key corresponding to a key information IK may be confirmed.

The ticket issuing means 450 includes an authentication information generating means 151, and issues a ticket containing an address A_U allocated by the address allocating means 140, a user identifier ID_U allocated by the user identifier allocating means 130, key information transmitted from the user terminal 500 together with the user authentication information, and authentication information IA generated by the authentication information generating means 151. In this manner, the ticket provides a correspondence between the user identifier and a key information. Thus, the authenticated user corresponds to a user terminal which keeps the private key associated with the key information. The ticket may contain a time stamp when the ticket has been issued, an effective period of the ticket, a communication band width allocated to the user terminal 500 and information relating to an access point 30 which covers the user terminal 500. An example of the ticket 53 is shown in Fig. 15. The ticket 53 is distinct from the ticket 51 used in the first mode in that the ticket 53 contains key information.

[0053] Upon a successful user authentication in response to an authentication request, the authentication server 400 allocates a user identifier to the user, and also allocates an address to an user terminal which corresponds to the user identifier. This address is set up as a source address in the user terminal 500 in the similar manner as in the first mode. Since the key information is associated with the public key of the user terminal 500, it follows that the authentication server 400 has made a user authentication by linking the user and the user terminal 500 utilized by the user (as a pair) by the key information, and the user terminal having the key information is allocated with the address.

[0054] According to the second mode, a user key pair for the user authentication is distinct from a terminal key pair for establishing a session, and the user key pair is held by an authentication device which is connected to the user terminal, whereby a user terminal located anywhere can be utilized by connecting the authentication device thereto. As a method of user authentication, a method which does not utilize the key pair may also be used.

[Second mode] user terminal

Fig. 13 is a block diagram of a user terminal which is used in the second mode for carrying out the present invention. The user terminal 500 comprises a communication interface 201 and control processing means 502. The control processing means 502 comprises a control unit 502a including a CPU for processing a program, a memory for storing the program and the like, an authentication request means 503, and a service request means 530. It should be understood that these means may be constructed by the modules of the program. The authentication request means 503 includes a user authentication information entry means 510, a user authentication information transmitting means 220 and a ticket reception means 231.

[0055] The user authentication information entry means 510 causes an authentication devices 41 to enter user authentication information and the like. The private key of the user key pair which is stored in the authentication device 41 cannot be taken out of the authentication device 41. The authentication device 41 may comprise a smart card, a hardware authentication token including USB (Universal Serial Bus) key, or a biometrics authentication device. Alternatively, a password/user name may be entered through an entry instrument 40 to be fed to a user authentication information generator 210 to generate user authentication information. Where the authentication device 41 is not connected to the user terminal 500 in a simplified arrangement, a terminal key pair stored in a key storage 502b may be used in place of the user key pair to generate user authentication information.

[0056] A key information generator 503a causes the public key of the user terminal 500 to be entered from a key storage 502b to generate key information. The key information generator 503a may deliver the entered public key directly as key information. A user authentication information transmitting means 220 transmits not only the user authentication information but also the key information to the authentication server 400 for purpose of an authentication request.

The service request means 530 comprises a session establishing means 532 and a packet cryptographic processing means 533, and is used to request a service provided by the application server 600. The session establishing means 532 generates in a session key generator 532a a secret key which is shared with the application server 600 as a session secret key K_{CUS} from a private key K_{SS} which forms a pair with an public key associated with the key information contained in the ticket 53 and the public key K_{PS} of the application server 600 in conformity to IKE (Internet Key Exchange).

[0057] After the session secret key has been shared by the application server 600, or after the secret key shared with the user terminal 500 is also generated as a session secret key in the application server 600, the packet cryptographic processing means 533 calculates an authentication header to transmitted packet information in an authentication header generator 533a, using the session secret key which is shared with the application server 600 by the session establishing means 532 in conformity to IPsec (Security architecture for the Internet Protocol) or TLS (Transport Layer Security) and adds the authentication header AH to the packet being transmitted. The authentication header generator 533a generates the authentication header by calculating one-way hash function with respect to the packet using the session secret key, thus allowing a recognition of whether or not the packet has been forged. The packet cryptographic processing means 533 may encrypt the packet in conformity to IPsec or TLS in an encryptor 533a' as indicated in parentheses in Fig. 13. Alternatively, the packet 54 can be added with the authentication header AH, and the resulting packet may be encrypted in the encryptor 533a'. The addition of the authentication header AH plus the cryptographic processing of the packet is generically referred to as a packet cryptographic processing, and an arrangement which performs such processing is referred to as a packet cryptographic processing means.

[0058] An example of construction of a packet 54 generated by the packet cryptographic processing means 533 is shown in Fig. 16. As a distinction from the packet 52 shown in Fig. 6, the header 54h is added with an authentication header and a ticket 53 in a payload 54p is added with a key information. It is to be noted that a packet may be encrypted in the encryptor 532b and added with the authentication header AH.

[Second mode] application server

Fig. 14 is a block diagram of an application server used in the second mode for carrying out the present invention. An application server 600 comprises a communication interface 301 and control processing means 602. The control processing means 602 comprises a control unit 602a including a CPU which processes a program, a memory which stores the program and the like, a service providing means 610, a session establishing means 611 and a ticket memory means 330. It is to be noted that these means may be constructed by modules of the program.

[0059] The service providing means 610 comprises an address comparison means 312 and a packet authentication means 612, and provides a service which is requested by the user terminal 500.

The session establishing means 611 includes a ticket verifying means 620, and establishes a session with the user terminal 500. In a procedure which establishes the session, it shares a session secret key with the user terminal 500 in conformity to IKE or the like. Thus, the session establishing means 611 generates in a session key generator 611a a secret key which is shared with the user terminal 500 as a session secret key K_{CUS} by using a private key K_{SA} of the application server 600 stored in the key storage 602b and the public key K_{PU} of the user terminal 500.

[0060] After sharing the session secret key with the user terminal 500, the packet authentication means 612 verifies the authentication header AH which is added to the received packet 54 using the session secret key K_{CUS}. If a result of verification of the authentication header which is added to the packet 54 is correct, the packet authentication means 612 delivers the ticket (CK2) 53 in the packet 54 to the ticket verifying means 620. When the received packet 54 is encrypted by the user terminal 500, a packet decrypting means 612' indicated in parentheses is used instead of the packet authentication means 612, and the packet 54 is decrypted with the session secret key K_{CUS}. When properly decrypted or when the packet 54 has not been forged, the decrypted packet 54 is delivered to the ticket verifying means 620. The authentication of the authentication header AH plus the decrypting processing of the packet 54 is generically referred to as a packet verification, and an arrangement to perform such verification is referred to as a packet verifying means.

[0061] The ticket verifying means 620 verifies the authenticity of the ticket 53 which is delivered by the packet authentication means 612. By way of example, the ticket verifying means 620 collates key information IK contained in the ticket 53 against the public key on the user side which is used when sharing the session secret key K_{CUS} in a key collator 620a, and if a matching therebetween applies, and in this example, if the address A_U contained in the ticket 53 is found to coincide with the source address A_S of the packet 54 when collated in an address collator 320b, this fact is detected by a memory command unit 620c, allowing the ticket (CK2) 53 to be stored in the ticket memory means 330. After the session with the user terminal 500 has been established and the ticket (CK2) 53 has been stored in the ticket memory means 330, when a service request packet is received from the user terminal 500 through the session, the service providing means 610 transmits a packet which allows the service requested by the user terminal 500 to be provided through the session of the user terminal 500 when the address comparison means 312 determines that the source address of the packet 54 which has been confirmed (or decrypted) by the packet authentication means 612 (or packet decrypting means 612') as not having been forged in conformity to IPsec or TLS and the like coincides with the address contained in the corresponding ticket (CK2) 53 which is stored in the ticket memory means 330. If required, the ticket verifying means 620 may include various verifiers such as the authentication information verifier 320a which can be provided in the ticket verifying means 320 shown in Fig. 4, in the similar manner as in the application server 300 used in the first mode.

[0062] [Second mode] processing procedure of authentication system

A processing procedure of the address based processing system according to the second mode for carrying out the present invention will be described below with reference to Fig. 17.

(1) Initially, the user terminal 500 generates user authentication information and key information IK, and transmits an authentication request to the authentication server 400 through the access point 30.

(2) Upon receiving the authentication request, the authentication server 400 performs an authentication of the user on the basis of the user authentication information, and upon a successful authentication of the user, allocates the user identifier ID_U and allocates the address A_U to the user terminal which corresponds to ID_U, and generates authentication information if required, issues a ticket 53 containing the user identifier ID_U, the address A_U, and the key information IK,

(3) and transmits the ticket to the user terminal 500.

[0063] (4) The user terminal 500 sets up the address A_U of the received ticket as a source address,

(5) the user terminal 500 calculates a session secret key K_{CUS} which is shared with the application server 600 by using its own private key K_{SU} and the public key K_{PS} of the application server 600 in conformity to a key exchange procedures such as IKE. It then generates an authentication header AH for the packet which is to be transmitted to the application server 600 using the session secret key K_{CUS}, allowing the header to be added to the packet. In the process of establishing a session, it transmits a packet including the authentication header and the ticket to the application server 600. By a procedure mentioned above, it requests the application server 600 to establish a session.

[0064] (6) In the process of establishing a session, the application server 600 calculates the session secret key K_{CUS} using its own private key K_{SS} and the public key K_{PU} of the user terminal, and uses the session secret key K_{CUS} to verify the authentication header AH which is added to the packet, and if required, also verifies the authentication information IA contained in the ticket (CK2) 53 which is received in the process of establishing a session using the shared secret key K_{CAS} with the authentication server 400. It also verifies whether or not the key information contained in the received ticket 53 corresponds to the public key on the user side (user public key or terminal public key) K_{PU} which is used in the calculation of the session secret key K_{CUS}, and collates the source address A_S of the received packet 54 against the address A_U contained in the ticket (CK2) 53, and if both of these verifications are successful, it stores the ticket (CK2) 53, thus establishing a session.

[0065] (7) In order to protect the source address A_S, the user terminal 500 performs at least one of the cryptographic processing which uses the session secret key K_{CUS} and the authentication header addition, and then it transmits a packet representing a service request to the application server 600 through the established session.

(8) The application server 600 decrypts the service request packet with the session secret key K_{CUS} or verifies the authentication header, determines whether or not the address contained in the stored ticket 53 coincides with the source address A_S of the packet which represents the service request, and upon coincidence of addresses, transmits packets which are effective to provide the service to the user to the user terminal 500.

[0066] [Second mode] processing by the authentication server

Fig. 18 is a flow chart showing a flow of processings by the authentication server which is used in the second mode for carrying out the present invention.

Upon receiving the authenticaiton request from the user terminal 500 (S101), an authentication of the user is performed by the authentication means 120 on the basis of the user authentication information, and upon a successful authentication of the user, the operation proceeds to S103 while if the authentication of the user fails, the operation is terminated (S102). The ticket 53 containing the address A_U, the user identifier ID_U and a key information IK is issued by the ticket issuing means 450 (S402). Other processings remain similar as in the processing procedure of the authentication server according to the first mode.

[0067] [Second mode] processings by the user terminal

Fig. 19 is a flow chart showing a flow of processings by the user terminal used in the second mode for carrying out the present invention.

In the processing of the user authentication request shown in Fig. 19A, user authentication information and key information IK are entered by the user authentication information entry means 510 (S501), and are transmitted by the user authentication information transmitting means 220 to the authentication server 400 through the communication interface 201 (S202). The ticket (CK2) 53 which is transmitted from the authentication server 400 is received by the ticket reception means 231 (S203).

[0068] In a subsequent processing shown in Fig. 19B where a session with the application server 600 is established, this processing is initiated by the session establishing means 532, sharing the session secret key between the user terminal 500 and the application server 600. The authentication header addition processing and/or cryptographic processing is applied to the packet 54 including the ticket 53 by the packet processing means 533, and the packet is transmitted to the application server 600 (S502).

After the session with the application server 600 has been established, the packet representing the service request is transmitted by the service request means 530 to the application server 600 through the establishing session, thus requesting the service to the application server 600 (S205).

[0069] [Second mode] processings by the application server

Fig. 20 is a flow chart showing a flow of processings by the application server used in the second mode for carrying out the invention.

Initially, the establishment of the session with the user terminal 500 is initiated by the session establishing means 611, and the session secret key which is obtained by a calculation from the own private key and the other party's public key in conformity to a key exchange procedure such as IKE is shared between the user terminal 500 and the application server 600 (S601). The packet 54 including the ticket 53 which is transmitted from the user terminal 500 is now received by the application server 600.

[0070] The authentication header which is added to the received packet 54 is verified by the packet authentication means 612 using the session secret key, and if the verification reveals that the packet 54 is not forged, but is authentic, the operation proceeds to S603. However, when the verification reveals that the packet 54 is not authentic as by being forged, the operation is terminated (S602). If the packet 54 is encrypted, it is decrypted by the packet decrypting means 612' using the session secret key, and when it is properly decrypted, the operation proceeds to S603.

When the authenticity of the ticket 53 is verified or when at least a matching between the key information contained in the ticket 53 and the public key on the user side which is used in sharing the session secret key is verified, and the source address A_S of the packet 54 coincides with the address A_U contained in the ticket (S603), the ticket 53 is determined to be authentic and is stored in the ticket memory means 330 (S303).

[0071] After the session has been established, the packet verifying means verifies whether or not the packet transmitted from the user terminal 500 and requesting a service is not forged and is authentic (S604), and if it is authentic, whether or not the source address of the packet coincides with the address contained in the stored ticket 53 is determined. Upon a coincidence between the addresses (S304), the service providing means 610 provides a service to the user through the user terminal 500 (S305).

A timing when the user terminal 500 transmits the packet 54 including the ticket 53 to the application server 600 may precedes the completion of the key exchange procedure such as IKE. In this instance, prior to the key exchange procedure, it is possible to determine beforehand whether or not the key exchange procedure is to be executed by verifying the ticket 53 transmitted from the user terminal 500 by the ticket verifying means 620. In this manner, an advantage is gained that a processing against an improper service request from a user terminal which does not have a ticket can be excluded at an early stage. However, because the transmission of the packet 54 including the ticket 53 takes place before the session secret key is shared between the user terminal 500 and the application server 600 and thus the packet verifying means cannot function, it follows that the detection of any forgery of the packet 54 cannot be made and there remains the possibility of a tort such as a replacement of the ticket. However, since the authentication information contained in the ticket 53 allows the ticket verifying means 620 to detect any forgery of the ticket 53 itself, when this is combined with verifying a matching between the public key on the user side which is used during the key exchange and the key information contained in the ticket 53, a confirmation that the ticket is transmitted from an authentic user terminal can be made. In other words, if the user terminal 500 transmits the ticket 53 to the application server 600 before the completion (immediately before or during) the key exchange procedure, the security can be finally maintained.

[0072] As described above, in the address based authentication system according to the second mode for carrying out the present invention, the authentication server transmits, on the basis of a result of the user authentication which takes place through the user terminal, a ticket which guarantees a correspondence between the user identifier, the address and the key information to the user terminal, the user terminal transmits the ticket to the application server and establishes a session therewith by sharing the session secret key and requests a service to the application server through the session, and the application server stores the ticket after confirming the authenticity of the received ticket, verifies the service request by collating the source address of the received service request packet and the address contained in the stored ticket and provides a service when it is properly verified.

[0073] In particular, because when the user terminal 500 transmits a packet to the application server 600, information such as the authentication header which is calculated using the session secret key or the like and which is used to detect any forgery is added to the packet as it is transmitted and the application server 600 confirms that there is no forgery of the packet which is transmitted from the user terminal 500, it is possible to guarantee that there is no forgery of the packet 54 which is transmitted from the user terminal 500 to the application server 600 during the session. In other words, it is guaranteed that there is no forgery in the source address contained in the packet.

[0074] In the example mentioned above, in order for the application server to verify a matching between the information received from the user terminal, for example, the public key on the user side, and the key information contained in the ticket when the session is established, the established session can be related to the ticket. In addition, the ticket is issued by the authentication server on the basis of the user authentication which takes place through the user terminal to guarantee an association between the user identifier, the address and the key information, a correspondence between the user terminal having the key related to the key information and the user specified by the user identifier is guaranteed. Consequently, the established session and the ticket guarantee a correspondence between the source address and the user.

[0075] Furthermore, since the ticket is issued on the basis of the user authentication as mentioned above, the authenticity of the address contained in the ticket can be guaranteed. Also, the collation of the address contained in the ticket which is stored in the application server against the source address of the packet and a guarantee that there is no forgery of the source address of the packet in the established session guarantee the authenticity of the source address of the packet. As a consequence, the authenticity of the source address of the packet and the correspondence between the source address and the user are guaranteed, thus enabling the address based authentication.

[0076] It is to be noted that the guarantee of the authenticity of the address by the ticket, or the guarantee that this is an address issued to a properly authenticated user through a proper procedure is enabled because the function of authenticating the user, the function of issuing the address and the ticket generating function which guarantees an association therebetween are implemented by the same authentication server. The guarantee of the correspondence between the user and the terminal by the ticket is possible because at the same time as the user authentication which takes place through the user terminal, the correspondence between the user and the terminal is determined by the procedure and the arrangement by which the key information is transmitted from the user terminal to the authentication server.

[0077] The correspondence between the user, the terminal and the address can be invalidated by erasing the private key relating to the key information from the terminal. This is because the key exchange is impossible without the private key, and if a different key is used, a matching with the key information contained in the ticket does not apply, resulting in both cases in a failure of establishing the session.

[Second mode] modification

The second mode is distinct from the first mode in a portion which relates to processings which utilize the key information IK. Accordingly, a modification described above in connection with the first mode is similarly possible in the second mode.

[0078] In the application server 600, the address collator 320b may be omitted, and when the key collator 620a confirms a matching, the ticket CK2 may be stored in the ticket memory means 330.

The key information IK is not limited to information relating to the public key of the user terminal. For example, where an authentication purpose shared secret key K_{US} is shared beforehand between the user terminal 500 and the application server 600, information which can prove the possession of the authentication purpose shared secret key K_{US} can be used. For example, as illustrated in a sequence diagram of Fig. 21A, upon a successful user authentication the authentication server 400 may generate a challenge b in a challenge generator 460 (Fig. 21B) and transmit it to the user terminal 500.

[0079] The user terminal 500, using a key information generator 503b' (Fig. 21C) in the authentication request means 503, calculates a value r of one-way hash function h for inputs b and the authentication purpose shared secret key K_{US}, $r=h(K_{US}, b)$ as a response to b received, and generates a pair of the challenge b and the response r as key information IK={b, r}. This key information IK is transmitted to the authentication server 400. It is to be noted that as the challenge b, instead of a value which is explicitly transmitted from the authentication server 500, an implicit challenge such as a time (time stamp) when the response is generated or a sequence number in the session may be used, and in this instance, the transmission and the reception of the challenge can be omitted.

[0080] The authentication server 400 confirms the authenticity of the challenge b contained in the received key information IK, and when it could confirm properly, it issues a ticket CK2 containing the key information IK. The authenticity of the challenge can be confirmed in a manner such that if the challenge b is an explicit one or is uniquely determined in dependence upon the session between the user terminal 500 and the authentication server 400, a coincidence therebetween is confirmed or if the challenge b is an implicit challenge such as a time t1 when the response r is calculated, the authenticity is confirmed by a requirement that a difference between t1 and time t2 when the ticket is issued is within a permissible range d (namely, $t2-t1 \leqq d$). An authentication in terms of the challenge and the response using a shared secret key is known in the art, and therefore a detailed description will not be given.

[0081] When establishing a session for purpose of a service request, the user terminal 500 which has received the ticket CK2 transmits the ticket CK2 to the application server 600 in the manner mentioned above.

In the application server 600, a terminal authenticator 620d (Fig. 21D) in the ticket verifying means 620 enters key information IK={b, r} to recalculate a hashed value (K_{US}, b) for the challenge b using the shared secret key K_{US}, collating in a collation decision unit whether or not the hashed value coincides with the response r within the key information IK. If a result of the collation indicates a coincidence, a command is issued from the collation decision unit of the terminal authenticator 620d to the memory command unit 620c (Fig. 14) to permit a storage, whereby the ticket is stored.

[0082] Alternatively, the terminal authenticator 620d (Fig. 21d) in the application server 600 may transmit an additional challenge b' in the process of establishing a session with the user terminal 500 to the user terminal, as indicated in broken lines in Fig. 21A, and receives a corresponding response r'=h(K_{US}, b') from the user terminal 500 for confirming the authenticity of r'. (In this instance, b' may be replaced by an implicit challenge)

By the above procedure, by confirming that the response r (r') to the challenge b (b') which is session dependent information is proper on the basis of the key information IK, the application server 600 can recognize that the user terminal 100 has possessed the shared secret key K_{US} at the time of the user authentication (and at the time of service request).

[0083] In addition, since the ticket CK2 is issued based on the user authentication, the correspondence between the key information IK, the address A_U and the user identifier ID_U is guaranteed and thus it can be guaranteed that the address A_U has been issued to the user terminal having the shared secret key K_{US} which is indicated by the key information. It can also be guaranteed that the service request which is made using the address A_U as the source is from the authenticated user. Further, it can be related to ID, name and home address or the like of the authenticated user.

The key information IK may be information which relates to the public key K_{PU} of the user terminal as indicated in the first example and may also be information which proves the possession of the authentication purpose shared secret key between the user terminal 500 and the application server

600. In sum, it may be the key information IK which enables the application server 600 to verify on the basis of the key information IK that the user terminal 500 possesses a private/secret key which enables the application server in general or the application server which received a service request to uniquely identify the user terminal 500, which is the private key K_{SU} of the key pair of the user terminal for the former and which is the authentication purpose shared secret key K_{US} for the latter.

[0084] The authentication servers shown in Figs. 2 and 12, the user terminals shown in Figs. 3 and 13 and the application servers shown in Figs. 4 and 14 may be each functioned by a computer. By way of example, an authentication server program which causes a computer to function as an authentication server shown in Fig. 2 may be installed into the computer from a record medium such as CD-ROM, a magnetic disk, a semiconductor memory medium or the like or may be downloaded through a communication network to cause the computer to execute the server program. The same applies for other instances.